Boletín de alerta

Boletín Nro.: 79
Fecha de publicación: 30/09/2025
Tema: Alerta 2025-79 Vulnerabilidad de Zero Day de escalación de privilegios en VMWare
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- VMware Aria Operations
- VMware Tools
- VMware Cloud Foundation
- VMware Telco Cloud Platform
- VMware Telco Cloud Infrastructure

Descripción

Recientemente se ha reportado una nueva vulnerabilidad de Día Cero (Zero Day) **que afecta tanto a VMware Tools** (incluyendo open-vm-tools en Linux) **como a VMware Aria Operations.** Si se explota con éxito la escalada de privilegios locales, los usuarios sin privilegios pueden ejecutar código en contextos privilegiados (p. ej., root). La vulnerabilidad ha sido identificada como **CVE-2025-41244** con un score CVSSv3 7.8 con criticidad Alta. Esta vulnerabilidad esta activa y está siendo explotada desde Octubre 2024 atribuida al grupo UNC5174.

La raíz del problema es que los scripts de “service discovery” pueden llegar a invocar binarios no confiables en rutas escribibles por usuarios no privilegiados durante la identificación de versiones de servicios, afectando tanto el modo con credenciales (Aria Operations) como el modo sin credenciales (VMware Tools).

La explotación exitosa de CVE-2025-41244 puede detectarse fácilmente mediante la monitorización de procesos secundarios poco comunes, como se muestra en los árboles de procesos anteriores. Al tratarse de una escalada de privilegios local, el abuso de CVE-2025-41244 indica que un adversario ya ha obtenido acceso al dispositivo afectado y que *se deberían* haber activado otros mecanismos de detección.

Dado que ya hay reportes de explotación activa de dicha vulnerabilidad y de PoC publicados, esto incrementar el riesgo de que dicha vulnerabilidad pueda ser utilizado en tareas post-explotación, recomendamos tomar medidas al respecto lo más pronto posible.

Mitigación:

- Deshabilitar el Service Discovery Management Pack (SDMP) y/o el “service discovery” sin credenciales en entornos sensibles, y reducir la frecuencia o alcance de estos recolectores donde sea viable.
- Endurecer el sistema: montar ***/tmp*** con ***noexec,nodev,nosuid;*** monitorear procesos hijo inusuales de ***vmtoolsd*** y scripts de ***get-versions.sh***
- Alertar sobre ejecuciones desde rutas temporales (p. ej., /tmp/*) y sobre procesos iniciados por VMware Tools/Aria que llamen binarios fuera de */usr/bin o /usr/sbin;*
- Revisar artefactos bajo ***/tmp/VMware-SDMP-Scripts-{UUID}/*** en entornos sin telemetría. Dado que es una LPE, su explotación indica compromiso previo: priorizar búsqueda de actividad de acceso inicial y otras señales de intrusión.

Solución:

El equipo VMware lanzó parche de seguridad para los diversos productos afectados, en la siguiente tabla se puede encontrar más información al respecto:

Producto	Version afectada	Version corregida
VMware Cloud Foundation VMware vSphere Foundation	9.x.x.x	9.0.1.0
VMware Cloud Foundation VMware vSphere Foundation	13.x.x.x [2]	13.0.5.0
VMware Aria Operations	8.x	8.18.5
VMware Tools	13.x.x	13.0.5
VMware Tools	12.x.x, 11.x.x	12.5.4
VMware Cloud Foundation	5.x, 4.x	KB92148
VMware Telco Cloud Platform	5.x, 4.x	8.18.5
VMware Telco Cloud Infrastructure	3.x, 2.x	8.18.5

Información adicional:

- https://cwe.mitre.org/data/definitions/267.html
- https://blog.nviso.eu/2025/09/29/you-name-it-vmware-elevates-it-cve-2025-41244/
- http://support.broadcom.com/group/ecx/support-content-view/-/support-content/Security%20Advisories/VMSA-2025-0015–VMware-Aria-Operations-and-VMware-Tools-updates-address-multiple-vulnerabilities–CVE-2025-41244-CVE-2025-41245–CVE-2025-41246-/36149
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149